A Thermodynamic Assessment of the Cyber Security Risk in Healthcare Facilities

Filipe Fernandes[1], Victor Alves[2], Joana Machado[3],
Filipe Miranda[4], Dinis Vicente[5], Jorge Ribeiro[2],
Henrique Vicente[6,7], and José Neves[1,7($\boxtimes$)]

[1] CESPU – Escola Superior de Saúde do Vale do Ave,
Vila Nova de Famalicão, Portugal
fernandes.filipe.fa@gmail.com

[2] Escola Superior de Tecnologia e Gestão, ARC4DigiT – Applied Research
Center for Digital Transformation, Instituto Politécnico de Viana do Castelo,
Viana do Castelo, Portugal
victoralves.at.vnc@gmail.com, jribeiro@estg.ipvc.pt

[3] Farmácia de Lamaçães, Braga, Portugal
joana.mmachado@gmail.com

[4] Administração Tributária e Aduaneira, Viana do Castelo, Portugal
luisfilipedearaujomiranda@gmail.com

[5] Escola Superior de Tecnologia e Gestão de Leiria,
Instituto Politécnico de Leiria, Leiria, Portugal
dinisvicente98@gmail.com

[6] Departamento de Química, Escola de Ciências e Tecnologia,
REQUIMTE/LAQV, Universidade de Évora, Évora, Portugal
hvicente@uevora.pt

[7] Centro Algoritmi, Universidade do Minho, Braga, Portugal
jneves@di.uminho.pt

Abstract. Over the last decades a number of guidelines have been proposed for best practices, frameworks, and cyber risk assessment in present computational environments. In order to improve cyber security vulnerability, in this work it is proposed and characterized a feasible methodology for problem solving that allows for the evaluation of cyber security in terms of an estimation of its entropic state, i.e., a predictive evaluation of its risk and vulnerabilities, or in other words, the cyber security level of such ecosystem. The analysis and development of such a model is based on a line of logical formalisms for Knowledge Representation and Reasoning, consistent with an Artificial Neural Networks approach to computing, a model that considers the cause behind the action.

Keywords: Entropy · Cyber security · Logic Programming · Knowledge Representation and Reasoning · Artificial Neural Networks